Unrecognized Operations and the Banks' Duty of Security: Case Studies at Indecopi

Patricia Uceda, Dr. [1]; Luis Polo, Mg. [1]; Grecia Adrianzén [1];
[1] *Universidad Privada del Norte, Perú,* patricia.uceda@upn.edu.pe, luis.polo@upn.edu.pe, N00352767@upn.pe

***Abstract* – This research analyzed the incidence of unrecognized operations in the financial system of northern Peru between 2018 and 2021, with an emphasis on credit cards (54.8%) and savings accounts (29.8%). Through a quantitative-descriptive approach, more than 2800 complaints reported to Indecopi were processed. The results show that 90% of the sanctions were directed at the financial system, with BCP, Interbank and Banco Azteca being the most denounced entities. The measures adopted were mostly reactive and uneven, without a unified technological strategy. Improvement strategies inspired by international experiences were proposed, including biometric authentication, artificial intelligence for transaction monitoring and an interbank anti-fraud network. It is also suggested to integrate digital security content into the school curriculum as a preventive measure. The study shows the need to articulate technology, regulation and education to strengthen financial customer protection and reduce operational risk.**

***Keywords*— Unrecognized transactions, consumer protection, financial institution, security**

Operaciones no reconocidas y el deber de seguridad de los bancos: Estudio de casos ante Indecopi

Patricia Uceda, Dr. [1]; Luis Polo, Mg. [1]; Grecia Adrianzén [1];
[1] *Universidad Privada del Norte, Perú,* patricia.uceda@upn.edu.pe, luis.polo@upn.edu.pe, N00352767@upn.pe

Resumen – Esta investigación analizó la incidencia de operaciones no reconocidas en el sistema financiero del norte del Perú entre 2018 y 2021, con énfasis en tarjetas de crédito (54.8 %) y cuentas de ahorro (29.8 %). A través de un enfoque cuantitativo-descriptivo, se procesaron más de 2800 denuncias reportadas ante Indecopi. Los resultados muestran que el 90 % de las sanciones se dirigieron al sistema financiero, siendo BCP, Interbank y Banco Azteca las entidades más denunciadas. Las medidas adoptadas fueron mayoritariamente reactivas y desiguales, sin una estrategia tecnológica unificada. Se propusieron estrategias de mejora inspiradas en experiencias internacionales, incluyendo autenticación biométrica, inteligencia artificial para monitoreo de transacciones y una red interbancaria antifraude. Asimismo, se sugiere integrar contenidos de seguridad digital en el currículo escolar como medida preventiva. El estudio evidencia la necesidad de articular tecnología, regulación y educación para fortalecer la protección al cliente financiero y reducir el riesgo operativo.

Palabras clave— Operaciones no reconocidas, protección al consumidor, entidad financiera, seguridad

I. INTRODUCCIÓN

A. Realidad problemática

La crisis sanitaria generada por la COVID-19 impactó no solo en el sector salud, sino también a nivel social y económico. Aunque el sistema financiero ya ofrecía servicios digitales, la nueva realidad intensificó su uso, exigiendo escenarios más seguros para los ciudadanos.

La evolución de las tecnologías de información y comunicaciones (TIC) modificó el comportamiento de consumo en sectores como el trabajo, la educación y las finanzas, motivando a muchas industrias a evaluar sus riesgos cibernéticos y establecer planes de mitigación [1].

La INTERPOL ha advertido que las estafas en línea son un peligro global creciente, impulsadas por tecnologías emergentes como inteligencia artificial, criptomonedas, phishing y ransomware, que afectan tanto a usuarios expertos como inexpertos [2].

En América Latina, el 92% de las entidades bancarias reportaron eventos de seguridad digital; el 37% sufrió ataques exitosos que incluyeron transacciones no reconocidas y fraudes cibernéticos. La ciberseguridad fue identificada como la prioridad principal [3].

El fraude bancario digital en la región mostró un aumento del 113% en malware móvil, facilitando accesos no autorizados a aplicaciones bancarias a través de smartphones, que representan entre el 70% y el 88% del total de líneas móviles en países como Perú, Colombia y Brasil. El costo asociado es aproximadamente 4.59 veces el valor de la transacción perdida, siendo los canales digitales responsables de más del 50% de las pérdidas generales [4].

En Europa, estafas por phishing, ataques a apps móviles y fraudes en banca en línea se han vuelto comunes. Para 2025, el fraude financiero digital a nivel global generó pérdidas superiores al billón de dólares. En América Latina, más del 50% de estas pérdidas provienen de canales digitales [4].

En países como Reino Unido, Estados Unidos y miembros de la Unión Europea, las pérdidas por fraudes bancarios han alcanzado cifras alarmantes. Se estima que las pérdidas ascienden a £485 millones en el Reino Unido, $2.8 mil millones en Estados Unidos y €1.2 mil millones en la Unión Europea. Entre las técnicas más utilizadas por los delincuentes se encuentran el phishing, el vishing, el malware, las estafas sentimentales y diversas formas de manipulación psicológica. Estos mecanismos logran que la víctima autorice pagos de manera consciente, lo que complica significativamente los procesos de recuperación del dinero por parte de las entidades financieras y deja a los usuarios en situación de alta vulnerabilidad [5].

Según reportes del Banco Central de Reserva del Perú y diversas entidades Fintech, el sector financiero ha tenido un crecimiento significativo en el uso de transacciones digitales, lo que plantea nuevos retos en materia de seguridad y protección del usuario. En el año 2024, en el Perú, se registraron 442 pagos digitales por adulto que, refleja la creciente confianza en la digitalización financiera pero también la urgencia de fortalecer las estrategias de interoperabilidad entre plataformas y sistemas [6].

Ante la falta de transparencia en la provisión de servicios, distintos países han fortalecido sus marcos regulatorios. Destacan la ACCC (Australia), la Dirección Nacional de Defensa del Consumidor (Argentina) y la PROFECO (México), que promueven entornos comerciales más justos [7].

En el Perú, corresponde al Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual la protección de los derechos del consumidor dentro de los alcances de la Ley N.º 29571, "Código de Protección y Defensa del Consumidor" [8]. Así se tiene que, cuando un cliente detecta un cargo no consumido, tiene derecho a presentar un reclamo, correspondiendo al proveedor responder en un máximo de 15 días hábiles sin posibilidad de prórroga [9].

En un entorno de crecimiento de servicios digitales, es importante analizar el marco normativo que regula las relaciones entre consumidores, proveedores y plataformas. Las operaciones no reconocidas y fraudes ya no son hechos aislados, sino fenómenos estructurales que comprometen la estabilidad financiera. El derecho se presenta como un sistema adaptativo frente a la innovación tecnológica [10].

En Perú, se han implementado normas sobre ciberseguridad, responsabilidad empresarial y validación segura de transacciones. Entre 2021 y julio de 2023, Indecopi impuso 1,284 sanciones a entidades financieras por operaciones no reconocidas, en su mayoría vinculadas a tarjetas de crédito (59.6%) y cuentas de ahorro (34.9%) [11].

Entre 2021 y marzo de 2025, Indecopi sancionó a 271 proveedores con 2,891 medidas por operaciones no reconocidas, de las cuales el 90% (2,601) se aplicaron al sistema financiero. Las multas superaron las 3,978.8 UIT. Los productos más involucrados fueron tarjetas de crédito (54.8%) y cuentas de ahorro (29.8%) [12].

En los siguientes párrafos se muestran las principales normas que protegen a los usuarios en el mundo digital financiero. Destacando el Código de Protección y Defensa del Consumidor que en su artículo 19 seguido del artículo 104 establecen la responsabilidad del proveedor y la carga probatoria compartida ante reclamos de los consumidores [13].

La Resolución SBS N.º 6523-2013 que regula las tarjetas de crédito y débito, disponiendo medidas de monitoreo y validación para transacciones sospechosas, así como bloqueos preventivos [14] seguido de la Resolución SBS N.º 504-2021 aprueba el Reglamento de Ciberseguridad, exigiendo autenticación multifactor para acceso a canales digitales y operaciones sensibles, incluyendo OTP y notificaciones inmediatas al usuario [15].

Así también la Ley N.º 27444, Texto Único Ordenado de la Ley del Procedimiento Administrativo General, permite en su numeral 1.15 que las entidades administrativas puedan adoptar precedentes para fortalecer la coherencia y predictibilidad en sus decisiones, lo que resulta útil en reclamos por operaciones no reconocidas [16].

La Superintendencia de Banca, Seguros y AFP (SBS) ha emitido documentos que fortalecen la protección del consumidor ante fraudes digitales. Dan cuenta de ello, el Oficio N.° 12205-2024-SBS y el Oficio N.° 36482-2022-SBS los cuales fortalecen la ciberseguridad financiera y promueven prácticas operativas seguras [17] y recientemente el Oficio N.º 29418-2025-SBS que amplia los canales por los cuales se realizan operaciones financieras y la necesidad de fortalecer la seguridad operativa ante los riesgos emergentes del ecosistema financiero digital [17].

B. Problema

Ante este escenario, surge la necesidad de analizar la magnitud del problema en el contexto regional, evaluar la efectividad de las medidas implementadas por las entidades financieras y formular recomendaciones que fortalezcan la prevención, detección y atención de las operaciones no reconocidas. Esta investigación busca contribuir con evidencia empírica y propuestas viables mejorar la seguridad de las transacciones y salvaguardar los derechos del consumidor financiero en el país.

C. Objetivo general

Analizar la problemática de las operaciones no reconocidas reportadas en la zona norte del Perú, evaluando las medidas implementadas por las entidades financieras y proponiendo acciones de mejora que fortalezcan la protección al cliente y la gestión del riesgo operativo.

D. Objetivos específicos

1. Caracterizar los casos de operaciones no reconocidas reportados por clientes de entidades financieras en las regiones de Cajamarca, Piura, Lambayeque y La Libertad, durante el periodo 2018-2021.
2. Evaluar la eficacia de las medidas preventivas y correctivas adoptadas por las entidades financieras para mitigar operaciones no reconocidas.
3. Proponer estrategias de mejora orientadas a reforzar los mecanismos de autenticación, monitoreo y respuesta ante operaciones no reconocidas en el sistema financiero peruano.

II. MÉTODO

A. Tipo de investigación

La presente investigación es descriptiva según su finalidad, porque busca describir detalladamente las características de una situación, sin intentar establecer relaciones entre causa y efecto.

Por su carácter, es observacional indirecta, ya que se ha realizado el análisis de reportes brindados por el Indecopi - Perú. Además, se enmarca en el enfoque de estudio de casos múltiples, al examinar denuncias individuales contra diversas entidades bancarias, en contextos regionales distintos, para identificar patrones y evaluar el cumplimiento del deber de seguridad por parte de las entidades bancarias implicadas.

B. Población muestral

La población muestral estuvo compuesta por 2,891 denuncias por operaciones no reconocidas presentadas ante Indecopi entre los años 2018 y 2021, correspondientes exclusivamente a entidades del sistema financiero peruano. El análisis se centró en regiones del norte del país: Cajamarca, Piura, La Libertad y Lambayeque. Las denuncias involucraron productos como tarjetas de crédito, cuentas de ahorro. La fuente primaria fueron los reportes proporcionados por la Oficina Regional de Indecopi Cajamarca, los cuales fueron depurados y organizados para su análisis estadístico y documental. Esta muestra refleja de manera representativa las prácticas y deficiencias en seguridad bancaria de las entidades financieras denunciadas en dicho periodo.

C. *Técnicas e instrumentos de recolección de datos*

Se utilizó el análisis documental como técnica principal, mediante la exploración de los reportes de denuncias y apelaciones registrados ante Indecopi. Estos documentos, obtenidos a través de solicitud oficial, permitieron identificar acciones tomadas por las entidades financieras, tiempos de respuesta y reincidencias, elementos claves para el análisis de casos.

D. *Procedimiento*

Se siguieron los siguientes pasos metodológicos:

- Solicitud formal de información a Indecopi.
- Consolidación de bases de datos por región y año.
- Limpieza de datos, considerando la variabilidad de formatos según la sede regional.
- Clasificación y codificación de los casos por tipo de producto y entidad denunciada.
- Aplicación de técnicas estadísticas y visualización de patrones.
- Documentación de medidas de seguridad adoptadas por los bancos denunciados.
- Redacción de resultados, análisis comparativo entre casos y formulación de propuestas de mejora.

E. *Tratamiento de datos*

Se aplicaron herramientas de análisis de frecuencias, Pareto y gráficos comparativos por región, año, producto y tipo de entidad. El procesamiento se realizó con Microsoft Excel y SPSS. A nivel cualitativo, se desarrolló una matriz de indicadores clasificadores para valorar el cumplimiento del deber de seguridad en cada caso. Asimismo, se revisaron resoluciones administrativas, normativa emitida por la SBS y buenas prácticas internacionales en prevención del fraude financiero, que permitieron enriquecer el análisis de casos con enfoque comparado.

III. RESULTADOS Y DISCUSIÓN

A continuación, se muestran los resultados obtenidos luego de la investigación realizada:

Respecto al **objetivo específico 1**: Caracterizar los casos de operaciones no reconocidas reportados por clientes de entidades financieras en las regiones de Cajamarca, Piura, Lambayeque y La Libertad, durante el periodo 2018-2021, se puede evidenciar que durante los años 2018 y 2019 se registraron el mayor número de denuncias por parte de los usuarios de La Libertad y Lambayeque.

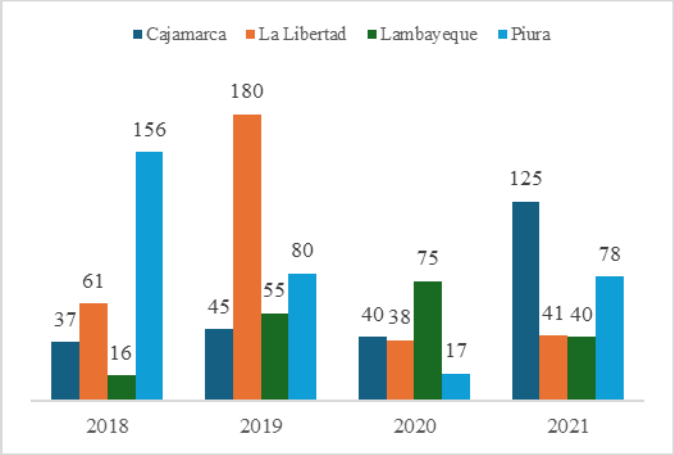

Fig. 1 Número total de operaciones no reconocidas registradas por sucursal y año - Indecopi

Según la Fig. 2, Piura encabeza la lista, representando aproximadamente el 31.5% de todos los casos registrados, lo que podría representar una alta vulnerabilidad o deficiencia de los mecanismos de validación y monitoreo de la zona. Continúa La Libertad, con un 27.6% acumulado adicional, alcanzando juntas casi el 60% del total de los casos y luego aparece Cajamarca, con un 24.7%, siendo Lambayeque con un 15.6% el que menor número de casos reportó

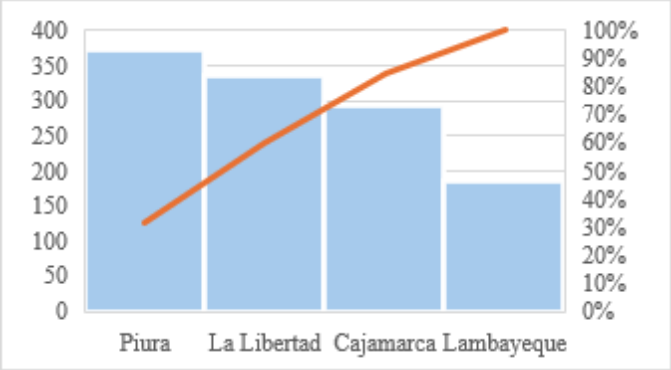

Fig. 2 Diagrama de Pareto - Frecuencia por sucursal de presentación

En la Fig. 2 se muestra también que el 80% acumulado se alcanza sólo con tres regiones (Piura, La Libertad y Cajamarca), lo cual indica que el esfuerzo de mitigación debiera enfocare específicamente en ellas. Piura representa por sí sola el tercio de total, lo que podría estar relacionado con: i) Alta presencia de productos financieros con débiles mecanismos de autenticación, limitada educación financiera y deficiencias en el monitoreo transaccional.

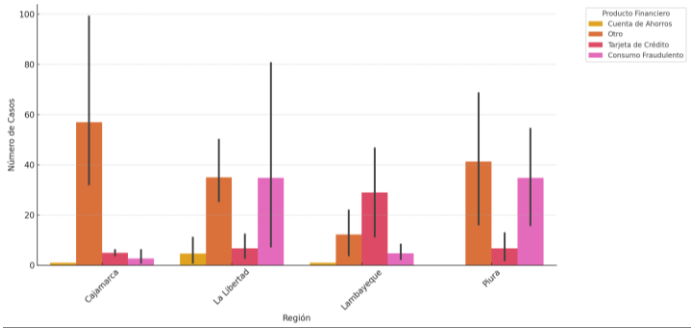

Fig. 3 Frecuencia de operaciones no reconocidas por producto financiero y región

Como se muestra en la Fig. 3 predomina la categoría Otro, lo cual indica una clasificación general que puede ocultar detalles específicos. Sin embargo, también se reporta un volumen importante de consumos fraudulentos, lo que sugiere que se deben revisar prácticas asociadas a fraudes con tarjetas y débiles mecanismos de autenticación en el canal digital.

En Trujillo, se observan niveles considerables de consumos fraudulentos y cuentas de ahorro, lo cual puede estar relacionado con phishing, smishing o accesos indebidos a través de banca por internet. Es una región donde se justifica fortalecer la educación financiera y mejorar los filtros antifraude.

En Cajamarca, la mayor parte de los casos se agrupa en la categoría Otro, aunque también destacan algunas denuncias por tarjetas de crédito. Este patrón sugiere la necesidad de revisar los protocolos de seguridad en establecimientos afiliados, así como la trazabilidad de los procesos de validación.

Mientras que, Lambayeque muestra una distribución más dispersa, con presencia significativa de consumos fraudulentos, lo que evidencia la urgencia de reforzar el monitoreo proactivo de operaciones inusuales, particularmente en puntos de venta físicos y digitales.

Respecto al **objetivo específico 2**: Evaluar la eficacia de las medidas preventivas y correctivas adoptadas por las entidades financieras para mitigar operaciones no reconocidas, se evaluaron resoluciones del Indecopi y SBS para conocer las medidas preventivas y correctivas que han ido implementando en orden cronológico.

Tal como se muestra en la Fig. 4, entre los 2019 y 2020, diversas entidades como: BCP, Interbank, BBVA y Oh! implementaron mecanismos de monitoreo transaccional, alertas tempranas y detección de fraudes informáticos [18], como medidas iniciales de control. Estas acciones respondieron a un incremento de reportes por consumos no reconocidos, especialmente en productos como tarjetas de crédito, reflejando un esfuerzo reactivo y fragmentado, para lo cual también devinieron luego reglamentaciones y nuevos procedimientos [12].

Fig. 4 Evolución de medidas implementadas

Durante el 2021 se produjo un momento clave: la Superintendencia de Banca, Seguros y AFP (SBS) emitió un reglamento que formaliza el uso obligatorio de autenticación reforzada en canales digitales, con énfasis en operaciones de riesgo. Esto obligó a los bancos a garantizar, por lo menos, el uso de dos factores de verificación independientes para validar la identidad de los usuarios. Desde el campo de la ingeniería de sistemas, esta norma implicó rediseñar las lógicas de acceso, adaptar las bases de datos de credenciales, y robustecer los sistemas de seguridad digital. Jurídicamente, el cambio marca una evolución hacia un modelo de corresponsabilidad técnica y legal, donde las entidades deben demostrar haber aplicado todos los mecanismos disponibles para proteger a sus clientes [19].

En el periodo 2023 - 2025, algunas entidades, como el Banco de la Nación y Scotiabank, empezaron a diferenciarse por adoptar prácticas más completas en cuanto a la gestión de operaciones no reconocidas [20]. Estas incluyeron sistemas de monitoreo en tiempo real, entrenamientos internos dirigidos a personal sobre fraude digital, y mecanismos de reversión automática de transacciones cuestionadas, todo ello en cumplimiento de mandatos establecidos en resoluciones administrativas del Indecopi. Estos casos reflejan no sólo una

respuesta ante sanciones previas, sino también un mayor compromiso con los principios de idoneidad y deber de seguridad establecidos en la normativa nacional. En otras palabras, se empieza a pasar de una lógica reactiva a una postura más anticipativa y coordinada entre los marcos técnicos y legales.

Resumiendo, aunque se ha avanzado hacia una mayor formalización de medidas de control, el análisis evidencia que aún persisten diferencias importantes entre entidades. Algunas prácticas clave como: la integración de algoritmos de inteligencia artificial para detectar anomalías, la capacitación continua del personal o la estandarización de la comunicación con el cliente, aún no se aplican en todas las entidades financieras. Esta falta de integración limita la efectividad general del sistema, tanto desde el punto de vista de la ingeniería de procesos como de la protección legal de los usuarios financieros.

TABLA I
FRECUENCIA DE MEDIDAS IMPLEMENTADAS POR ENTIDAD

Entidad	**Cantidad**			**Tiempo Promedio Plazo Correctivo (días)**	**% Devoluciones eficaz efectivas**
	Medidas Preventivas	**Tipos de Preventivas**	**Medidas Correctivas**		
Scotiabank	3	3	2	10–15	≥ 90 %
Banco de la Nación	2	2	2	15	Aprox. 100 %
BCP	2	2	1	-	-
Interbank, BBVA, Oh!	2	2	1	-	-

Como muestra la Tabla I, algunas entidades como Scotiabank y el Banco de la Nación han implementado medidas preventivas en varias capas, como autenticación reforzada, monitoreo en tiempo real y capacitación. Aunque no existe una estrategia uniforme de regularización, estas acciones reflejan un mayor compromiso con la gestión del riesgo operativo.

Ahora bien, al revisar el número de tipos de medidas preventivas implementadas, se ve con claridad que no basta con la cantidad: también importa la variedad. Desde la perspectiva del diseño de sistemas, implementar únicamente filtros de acceso no es suficiente si no se complementan con análisis de patrones, sistemas de alertas y protocolos de respuesta. De lo contrario, se generan puntos ciegos que los atacantes pueden explotar [21].

Por otro lado, el análisis no puede quedarse en la tecnología. Desde la mirada jurídica, el cumplimiento del deber de seguridad implica no sólo prevenir, sino también actuar con diligencia cuando el problema ocurre. En este punto, el indicador de medidas correctivas toma protagonismo. Instituciones que han incorporado mecanismos de reversión automática, o que han sido capaces de restituir montos en plazos razonables (como el Banco de la Nación), demuestran una comprensión más clara del principio de responsabilidad objetiva en la prestación de servicios financieros [19].

El tiempo promedio de respuesta, aunque no siempre público, resulta clave para medir la experiencia del usuario. Y más aún si se vincula con el porcentaje de devoluciones eficaces. Desde el punto de vista del derecho del consumidor, la carga de la prueba no debe recaer en el cliente; y desde la ingeniería, un sistema bien diseñado debe poder identificar con precisión cuándo una operación ha sido irregular y revertirla sin fricción [18].

Finalmente, lo que muestra la Tabla I es que aún existe una brecha entre lo que algunas entidades hacen por cumplimiento y lo que otras hacen por iniciativa y convicción. El análisis integrado de estos indicadores podría servir como base para proponer un sistema de certificación de buenas prácticas o incluso para modelar algoritmos predictivos que anticipen fallos sistémicos antes de que escalen a nivel legal o reputacional [22].

Finalmente, respecto a los resultados obtenidos para el **objetivo específico 3**: Proponer estrategias de mejora orientadas a reforzar los mecanismos de autenticación, monitoreo y respuesta ante operaciones no reconocidas en el sistema financiero peruano, se puede mencionar que:

Luego del análisis comparativo internacional, se observa en la Tabla II que países como Singapur, Canadá y la Unión Europea han logrado reducciones de fraude de entre 60 % y 70 %, implementando tecnologías como autenticación biométrica obligatoria en banca móvil y sistemas de monitoreo predictivo en tiempo real. Estos países combinan autenticación adaptativa, biometría y algoritmos de aprendizaje automático como parte de una arquitectura de defensa en profundidad [23].

TABLA II
ESTRATEGIAS INTERNACIONALES CONTRA FRAUDES FINANCIEROS

País / Región	Estrategia Clave	Reducción %	Fuente	Año
Singapur	Autenticación biométrica obligatoria en banca móvil	70	Monetary Authority of Singapore	2021
Reino Unido	Sistema de alerta nacional de fraudes (Take Five Campaign)	55	UK Finance	2022
Canadá	IA para análisis predictivo en tiempo real	65	Bank of Canada	2022
Unión Europea	PSD2: Autenticación fuerte del cliente (SCA)	60	European Banking Authority	2019
Chile	Normativa de ciberseguridad bancaria (NBSF-2022)	45	CMF Chile	2022
Australia	Plataforma de trazabilidad interbancaria antifraude	50	Australian Payments Network	2021

Los indicadores de la Tabla I muestran que, en el caso peruano, muchas entidades aún se limitan a medidas preventivas básicas: sobre todo monitoreo transaccional reactivo y alertas insuficientes. El número de medidas preventivas es bajo y, en ocasiones, poco diverso (Cantidad Tipos de preventivas), lo cual evidencia una arquitectura tecnológica con falencias en adaptabilidad y densidad de controles.

En cuanto a las medidas correctivas, algunas instituciones ya implementan procesos de reversión automática y plazos razonables de restitución al cliente. No obstante, los indicadores reflejan que permanecen grandes diferencias entre entidades: el tiempo promedio de respuesta suele exceder los límites razonables y el porcentaje de devoluciones eficaces varía significativamente. Mientras que en jurisdicciones como el Reino Unido los bancos como Barclays reportan tasas de devolución superiores al 90 % y plazos menores a una semana, otras instituciones alcanzan menos del 10 % de devolución efectiva [24].

Con base en estos indicadores y en las mejores prácticas internacionales, se propone que el Perú implemente estrategias prioritarias:

- Autenticación biométrica adaptativa para operaciones sensibles, cubriendo factores de conocimiento, posesión y biométricos. Beneficiaría directamente el indicador de Cantidad - Tipos de medidas preventivas.
- Monitoreo predictivo en tiempo real con inteligencia artificial, lo cual reforzaría la detección temprana y reducirá la necesidad de medidas curativas tardías, mejorando también el porcentaje de devoluciones eficaces.
- Plataforma interbancaria de trazabilidad, que permita compartir alertas entre entidades, anticipar fraudes y proteger eficientemente al cliente en la línea de espera.

Estas propuestas revelan que sólo una estrategia sistémica, colaborativa y supervisada puede acercar al Perú a estándares resilientes. Jurídicamente, esto implicaría elevar los requisitos mínimos de seguridad bajo el deber de idoneidad definido por la SBS e Indecopi, y transformar el cumplimiento normativo en una cultura organizacional proactiva, solidaria y transparente.

En referencia al objetivo general: Analizar la problemática de las operaciones no reconocidas reportadas en la zona norte del Perú, evaluando las medidas implementadas por las entidades financieras y proponiendo acciones de mejora que fortalezcan la protección al cliente y la gestión del riesgo operativo, se determinó:

El análisis consolidado de más de 2800 denuncias impuestas entre 2018 y 2021 en regiones del norte del Perú como Cajamarca, Piura, La Libertad y Lambayeque permitió identificar que las operaciones no reconocidas se concentran especialmente en productos como tarjetas de crédito (54.8 %) y cuentas de ahorros (29.8 %). Estas denuncias derivaron en sanciones económicas impuestas por Indecopi a entidades como BCP, Interbank, Banco Azteca y BBVA, reflejando una problemática sistemática de vulnerabilidad operativa y falta de control en las validaciones de identidad digital.

A partir del análisis estadístico por año, región y entidad denunciada, se observó que el 90 % de las sanciones impuestas por operaciones no reconocidas se concentró en el sistema financiero, con una tendencia creciente en regiones fuera de Lima. Destacan particularmente las sucursales de Piura y La Libertad por su alta frecuencia de denuncias, lo cual podría estar vinculado con brechas en infraestructura digital, niveles bajos de alfabetización financiera o deficiencias en la supervisión local de las entidades.

Respecto a las medidas preventivas y correctivas, el estudio identificó que, si bien algunas entidades financieras han mejorado sus sistemas de monitoreo y autenticación (como Interbank o Scotiabank), aún persisten brechas significativas en el uso de herramientas avanzadas como la inteligencia artificial, el monitoreo en tiempo real y la trazabilidad interbancaria. Los indicadores derivados de las tablas clasificadoras mostraron una implementación parcial y poco homogénea de medidas clave, lo cual debilita la capacidad del sistema para anticiparse a patrones de fraude y resolver con eficacia las operaciones no reconocidas reportadas por los clientes.

A partir de la comparación internacional, se propusieron estrategias concretas adaptables al contexto peruano, tales como la autenticación biométrica obligatoria, la creación de una red nacional de trazabilidad antifraude, y el establecimiento de un sello oficial de cumplimiento tecnológico y legal, inspirado en buenas prácticas de Singapur, Reino Unido y Chile

En conclusión, los resultados del estudio no sólo cuantifican la magnitud de la problemática, sino que permiten identificar patrones, carencias estructurales y puntos de mejora. Esto aporta evidencia técnica y jurídica que puede ser utilizada por los órganos reguladores (como la SBS e Indecopi) y por las propias entidades financieras para rediseñar sus sistemas de seguridad y atención al cliente, y avanzar hacia una gestión del riesgo operativo más integral, ética y centrada en la protección de los derechos del usuario financiero.

IV. CONCLUSIONES Y RECOMENDACIONES

Luego del análisis realizado, se puede concluir que:

Entre 2018 y 2021, las operaciones no reconocidas afectaron principalmente a usuarios de tarjetas de crédito (54.8 %) y cuentas de ahorro (29.8 %) en regiones del norte del Perú. El 90 % de las 2891 sanciones impuestas por Indecopi se dirigieron al sistema financiero, evidenciando deficiencias persistentes en mecanismos de seguridad y validación de identidad.

Se concluye también que, las acciones preventivas y correctivas implementadas por las entidades financieras han sido fragmentadas y, en muchos casos, reactivas. Pese a

avances como la autenticación reforzada en 2021, los indicadores muestran que no existe aún una respuesta sistémica homogénea frente al riesgo operativo.

Respecto a las oportunidades de mejora, se concluye que, inspirados en experiencias internacionales, se identificaron estrategias que el Perú podría adoptar, como: la autenticación biométrica, la inteligencia artificial en monitoreo y la trazabilidad interbancaria, con potencial de reducir los fraudes financieros en más del 60 % si se aplican con enfoque integral y colaborativo.

Finalmente, se concluye que, la problemática de las operaciones no reconocidas en la zona norte no es sólo técnica, sino también humana y legal. Resolverla requiere fortalecer tanto la arquitectura tecnológica como el cumplimiento normativo y el trato justo al cliente y la concientización tecnológica y financiera de los usuarios.

A continuación, se comparten algunas recomendaciones:

Se recomienda que las entidades financieras adopten métodos de autenticación basados en biometría (huella, reconocimiento facial, voz), complementados con factores de posesión (token, app) y conocimiento (PIN), especialmente en operaciones de alto riesgo como transferencias y compras en línea. Esta medida, común en países como Singapur y Canadá, no sólo refuerzan la seguridad, sino que mejora la experiencia del usuario, reduciendo su exposición a fraudes por suplantación.

Se recomienda la implementación de motores analíticos que utilicen inteligencia artificial para detectar patrones sospechosos, transacciones atípicas o conductas de riesgo en tiempo real. Esta tecnología ya ha sido probada en Canadá y Australia con resultados positivos, logrando reducciones superiores al 60 % en fraudes digitales.

El Perú requiere una red segura y compartida entre entidades financieras para identificar, alertar y bloquear transacciones potencialmente fraudulentas antes de que el daño se materialice. Esta herramienta debe estar integrada con los sistemas de la SBS y permitir la colaboración entre bancos, cajas y financieras.

Las soluciones tecnológicas deben ir acompañadas de formación al personal de atención al público y educación financiera al usuario. Se recomienda que las entidades realicen campañas masivas, accesibles y contextualizadas que expliquen cómo identificar intentos de fraude, cómo actuar, y cuáles son los derechos del cliente.

Desde el ámbito jurídico, se recomienda actualizar las normas para fijar plazos de atención, aplicar responsabilidad objetiva en casos de suplantación comprobada y establecer mecanismos eficaces de reversión de fondos, a fin de garantizar un trato justo y fortalecer la confianza del consumidor.

Se recomienda al Ministerio de Educación (MINEDU) y a las direcciones regionales de educación incluir en el currículo escolar (EBR), especialmente en secundaria, temas vinculados a la ciberseguridad personal, uso responsable de medios digitales, reconocimiento de intentos de fraude y derechos del consumidor financiero. Ya que una población escolar informada será, a futuro, una ciudadanía más preparada para enfrentar riesgos digitales como el phishing, los fraudes bancarios o las operaciones no reconocidas. Esta medida no solo fortalece la prevención, sino que contribuye a una alfabetización financiera y tecnológica temprana, esencial en un país donde el uso de banca digital se ha masificado aceleradamente tras la pandemia.

Y finalmente, se recomienda para futuras investigaciones ampliar la muestra que comprenda resoluciones emitidas por las 26 oficinas regionales de Indecopi entre los últimos 5 años, referente a las medidas de seguridad implementadas por las entidades del sistema bancario que, permita identificar el avance en la implementación de herramientas de inteligencia artificial para mitigar las denuncias frente a operaciones no reconocidas.

AGRADECIMIENTO

Nuestro agradecimiento a la Oficina Regional de Indecopi Cajamarca por haber facilitado el acceso a la información pública de denuncias y expedientes que han sido atendidos tras el hecho infractor de operaciones no reconocidas o falta de idoneidad de las oficinas de La Libertad, Piura, Lambayeque y Cajamarca.

REFERENCIAS

[1] M. FISA GROUP, “Ciberseguridad | Retos para el sector bancario este 2021,” Ciberseguridad | Retos para el sector bancario este 2021. [Online]. Available: https://www.fisagrp.com//blogs/ciberseguridad-reto-sector-bancario-2021

[2] “Evaluación de INTERPOL sobre estafas: un peligro mundial incrementado por la tecnología.” [Online]. Available: https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2024/Evaluacion-de-INTERPOL-sobre-estafas-un-peligro-mundial-incrementado-por-la-tecnologia

[3] Organización de los Estados Americanos and ASOBANCARIA, “Desafíos del riesgo cibernético en el sector financiero para Colombia y América Latina,” 2019. [Online]. Available: https://www.oas.org/es/sms/cicte/docs/Desafios-del-riesgo-cibernetico-en-el-sector-financiero-para-Colombia-y-America-Latina.pdf

[4] “El fraude ‘financiero digital’ acecha con fuerza en 2025 y estas son las principales tendencias en Latam,” InnovaciónDigital360. [Online]. Available: https://www.innovaciondigital360.com/pago-electronico/el-fraude-financiero-digital-acecha-con-fuerza-en-2025-y-estas-son-las-principales-tendencias-en-latam/

[5] “Análisis del Fraude Bancario Autorizado en 2025 | LinkedIn.” [Online]. Available: https://www.linkedin.com/pulse/an%C3%A1lisis-del-fraude-bancario-autorizado-en-2025-ironchip-eacwe/

[6] “Reporte del Sistema Nacional de Pagos y del sector Fintech en Perú - Marzo 2025.” [Online]. Available: https://www.bcrp.gob.pe/docs/Publicaciones/reporte-del-sistema-nacional-de-pagos/2025/marzo/rspf-marzo-2025.html

[7] Indecopi, “Indecopi - Por países.” Accessed: May 01, 2023. [Online]. Available: https://indecopi.gob.pe/web/biblioteca-virtual/pac-por-paises?p_p_id=101_INSTANCE_RxoOJZiYJrmx&p_p_lifecycle=0&

p_p_state=normal&p_p_mode=view&p_p_col_id=column-3&p_p_col_pos=1&p_p_col_count=2&_101_INSTANCE_RxoOJZiYJrmx_delta=20&_101_INSTANCE_RxoOJZiYJrmx_keywords=&_101_INSTANCE_RxoOJZiYJrmx_advancedSearch=false&_101_INSTANCE_RxoOJZiYJrmx_andOperator=true&p_r_p_564233524_resetCur=false&_101_INSTANCE_RxoOJZiYJrmx_cur=2

[8] Indecopi, "Autoridad Nacional de Protección del Consumidor - Indecopi." Accessed: May 01, 2023. [Online]. Available: https://www.consumidor.gob.pe/autoridad-nacional

[9] "Libro de Reclamaciones - Indecopi." Accessed: May 01, 2023. [Online]. Available: https://www.consumidor.gob.pe/libro-de-reclamaciones

[10] M. Castells, "Comunicación y poder," 2009.

[11] "Indecopi impone 1,284 sanciones a bancos por operaciones no reconocidas por clientes." [Online]. Available: https://elperuano.pe/noticia/221705-indecopi-impone-1284-sanciones-a-bancos-por-operaciones-no-reconocidas-por-clientes

[12] "Sistema financiero concentra el 90 % de sanciones por operaciones no reconocidas, revela Indecopi." [Online]. Available: https://www.gob.pe/institucion/indecopi/noticias/1150056-sistema-financiero-concentra-el-90-de-sanciones-por-operaciones-no-reconocidas-revela-indecopi

[13] "Ley N.° 29571." [Online]. Available: https://www.gob.pe/institucion/indecopi/normas-legales/1244218-29571

[14] Superintendencia de Banca y Seguros y AFP, "Resolución SBS No. 6523-2013," Oct. 2013. [Online]. Available: https://intranet2.sbs.gob.pe/intranet/INT_CN/DV_INT_CN/718/v11.0/Adjuntos/6523-2013.R%20.pdf

[15] Superintendencia de Banca y Seguros y AFP, "Resolución SBS No. 504-2021," Feb. 2021. [Online]. Available: https://intranet2.sbs.gob.pe/dv_int_cn/2046/v2.0/Adjuntos/504-2021.R.pdf

[16] "Ley N° 27444 Ley del Procedimiento Administrativo General – Sistema Peruano de Información Jurídica." Accessed: May 16, 2025. [Online]. Available: https://spijweb.minjus.gob.pe/sdm_downloads/ley-n-27444-ley-del-procedimiento-administrativo-general/

[17] Superintendencia de Banca, Seguros y AFP, "Oficio N° 29418-2025-SBS." Jun. 05, 2025. [Online]. Available: https://www.sbs.gob.pe/Portals/0/1-OFICIO-29418-2025-SBS-PL-10624.pdf

[18] Lex, "¿Las medidas de seguridad forman parte del deber de idoneidad en la prestación de servicios financieros?," LP. [Online]. Available: https://lpderecho.pe/medidas-seguridad-deber-idoneidad-prestacion-servicios-financieros/

[19] "Autenticación reforzada: mayor seguridad para operaciones que puedan generar perjuicio al usuario," SBSPerú. [Online]. Available: https://www.sbs.gob.pe/

[20] "Superintendencia de Banca, Seguros y AFP del Perú," SBSPerú. [Online]. Available: https://www.sbs.gob.pe/

[21] V. R. S. Llerena, "Lineamiento de seguridad bancaria para detectar y prevenir las operaciones bancarias no reconocidas o fraudulentas de las tarjetas de crédito o débito," LP. [Online]. Available: https://lpderecho.pe/lineamiento-seguridad-bancaria-detectar-prevenir-operaciones-bancarias-reconocidas-fraudulentas-tarjetas-credito-debito/

[22] "Indecopi multa al Banco de la Nación con más de S/18 mil por permitir operación no reconocida en perjuicio de una usuaria - Infobae." [Online]. Available: https://www.infobae.com/peru/2025/06/03/indecopi-multa-al-banco-de-la-nacion-con-mas-de-s18-mil-por-permitir-operacion-no-reconocida-en-perjuicio-de-una-usuaria

[23] J. R. McConvey, "Financial firms beef up fraud prevention with biometrics and FIDO standards | Biometric Update." [Online]. Available: https://www.biometricupdate.com/202506/financial-firms-beef-up-fraud-prevention-with-biometrics-and-fido-standards

[24] "Over £1.2 billion stolen through fraud in 2022, with nearly 80 per cent of APP fraud cases starting online," UK Finance. [Online]. Available: https://www.ukfinance.org.uk/news-and-insight/press-release/over-ps12-billion-stolen-through-fraud-in-2022-nearly-80-cent-app